

IN THE CLAIMS:

Please cancel claims 24-26, and amend the claims as follows:

1. (Currently Amended): A method for processing a fragmented packet with a firewalling device, comprising:
 - receiving fragments of the packet prior to processing of firewall policies at the firewalling device;
 - sorting the fragments according to the packet and order of the fragments;
 - storing the fragments in association with the packet and in order in a connection table (CT) and a Network Address Translation table (NT);
 - cross linking the NT and CT by storing a hash of at least a portion of the fragments in one of the NT and CT tables;
 - ~~reconstitute the packet~~
 - collecting and assembling all the fragments in order to fully reconstitute the packet prior to applying firewall policies; [[and]]
 - storing an Address Research Table (ART) for a first packet of a connection to the firewall device in association with one of the NT and the CT, and the hashing each of the subsequent packets to determine a table entry to forward the packet; and
 - transferring the packet to the firewalling device to apply the firewall policies to the entire packet at one time.
2. (Previously Presented): The method, according to claim 1, further comprising:
 - obtaining source and destination address information for the fragments; and
 - determining if the source and destination address information of the fragments matches of the other fragments.
3. (Original): The method, according to claim 1, further comprising determining if the fragments have a valid checksum.
4. (Original): The method, according to claim 1, wherein the sorting comprises obtaining packet and fragment identifiers.

5. (Original): The method, according to claim 4, further comprising determining if any of the fragments needed to reconstitute the packet have not been stored.
6. (Original): The method, according to claim 5, further comprising determining if the fragments stored collectively exceed a communication length threshold.
7. (Original): The method, according to claim 6, further comprising purging the fragments responsive to the communication length threshold being exceeded.
8. (Original): The method, according to claim 7, further comprising starting a timer in association with an initial one of the fragments received by the firewalling device.
9. (Original): The method, according to claim 8, further comprising checking whether all the fragments needed to reconstitute the packet have not been received to the firewalling device within a threshold time period.
10. (Original): The method, according to claim 1, wherein the storing comprises overwriting one of the fragments with a subsequently received fragment.
11. (Previously Presented): A computer readable medium containing a program which when executed by a processor which assembles a fragmented packet prior to processing by a stateful firewalling device, comprising:
 - obtaining fragments of the packet, each of the fragments having a packet identifier and a fragment identifier, each of the fragments have a source address and a destination address;
 - hashing at least a portion of the fragments obtained;
 - determining if the source address and the destination address is currently stored in a connection table at the stateful firewall in association with the packet identifier based on the hash;
 - reserving buffer memory space and starting a timer responsive to the source address and the destination address not being currently stored;
 - responsive to the source address and the destination address being currently stored, determining for each of the fragments subsequently received after receipt of an

initial fragment with the packet identifier whether a respective checksum for the fragments subsequently received is valid;

sorting the fragments according to the packet identifier and the fragment identifier;

storing the fragments to reconstitute the packet in the buffer memory space reserved to fully reconstitute the packet including all fragments in association with the packet identifier and in order according to the fragment identifier; and

transferring the fully reconstituted packet to the firewalling device to apply firewall policies to the entire fully reconstituted packet at one time.

12. (Previously Presented): The computer readable medium, according to claim 11, further comprising:

determining if all the fragments to reconstitute the packet have been stored; and reconstituting the packet according using the fragments stored for the packet.

13. (Previously Presented): The computer readable medium, according to claim 12, further comprising determining if any of the fragments needed to reconstitute the packet have not been stored.

14. (Previously Presented): The computer readable medium, according to claim 12, further comprising determining if the fragments stored collectively exceed a communication length threshold.

15. (Previously Presented): The computer readable medium, according to claim 14, further comprising clearing the buffer memory space reserved of any of the fragments responsive to the communication length threshold being exceeded.

16. (Previously Presented): The computer readable medium, according to claim 15, further comprising checking whether all the fragments needed to reconstitute the packet have not been obtained by the firewalling device within a threshold time period.

17. (Previously Presented): The computer readable medium, according to claim 16, further comprising clearing the buffer memory space reserved of any of the fragments responsive to the threshold time period being exceeded.

18. (Previously Presented): The computer readable medium, according to claim 12, wherein the packet is reconstituted prior to interrogation.
19. (Previously Presented): The computer readable medium, according to claim 11, wherein the fragments are physically stored in order within the buffer memory space reserved.
20. (Previously Presented): The computer readable medium, according to claim 11, wherein the fragments are logically stored in order within the buffer memory space reserved.
21. (Previously Presented): The computer readable medium, according to claim 11, wherein the fragments are Internet Protocol version four formatted packets.
- 22 – 27 (Cancelled)
29. (Currently Amended): The method of claim [[28]]_1, including comparing information from each received packet to the previous received packet before forwarding the packet.
30. (Previously Presented): The method of claim 1, wherein the hash function is based on the incoming packet 5-triple information.
31. (Previously Presented): The method of claim 30, wherein the input to the hash function of the NT index uses public address information.